**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**
**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**
**ВНУТРІШНІХ СПРАВ**

**Кафедра кібербезпеки та DATA-технологій, факультет № 6**

# МЕТОДИЧНІ МАТЕРІАЛИ ДО ПРАКТИЧНИХ ЗАНЯТЬ

з навчальної дисципліни
**«Управління та організація в сфері інформаційної безпеки»**

обов'язкових компонент
освітньої програми першого рівня вищої освіти

**"Кібербезпека" (Безпека інформаційних та комунікаційних систем)**

Харків 2023

**ЗАТВЕРДЖЕНО**
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

**СХВАЛЕНО**
Вченою радою
факультету № 6
Протокол від 25.08.2023 № 7

**ПОГОДЖЕНО**
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 (протокол від 15.08.2023 № 8).

**Розробники:**
Доцент кафедри кібербезпеки та DATA-технологій факультету № 6, кандидат наук з державного управління, доцент Онищенко Ю.М.

**Рецензенти:**
завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, доктор технічних наук, професор Петров К.Е.
доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент Світличний В.А.

## 1. Розподіл часу навчальної дисципліни за темами

| Номер та назва навчальної теми | Кількість годин, відведених на вивчення навчальної дисципліни | | | | | | Література | Вид контролю |
|---|---|---|---|---|---|---|---|---|
| | Всього | з них: | | | | | | |
| | | лекції | Семінарські заняття | Практичні заняття | Лабораторні заняття | Самостійна робота | | |
| **Семестр № 8** | | | | | | | | |
| Тема № 1. Основні положення щодо організації системи захисту інформації | **18** | **4** | | **6** | | **8** | **1-8** | **Залік** |
| Тема № 2. Визначення інформаційних ресурсів, що підлягають захисту | **18** | **4** | | **6** | | **8** | **1-8** | |
| Тема № 3. Виявлення повної множини загроз безпеки інформаційним ресурсам, які підлягають захисту | **18** | **4** | | **6** | | **8** | **1-8** | |
| Тема № 4. Проведення оцінки уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз | **16** | **4** | | **4** | | **8** | **1-8** | |
| Тема № 5. Методи та засоби захисту інформації | **16** | **4** | | **4** | | **8** | **1-9** | |
| Тема № 6. Захист інформації в комп'ютерних системах від несанкціонованого доступу | **16** | **4** | | **4** | | **8** | **1-8** | |
| Тема № 7. Політика інформаційної безпеки | **16** | **4** | | **4** | | **8** | **1-9** | |
| Тема № 8. Розробка проекту системи захисту інформації | **16** | **4** | | **4** | | **8** | **1-9** | |
| Тема № 9. Впровадження, визначення якості і управління системою захисту інформації | **16** | **4** | | **4** | | **8** | **1-9** | |
| Тема № 10. Нормативно-правова база США щодо забезпечення інформаційної безпеки | **16** | **4** | | **2** | | **10** | **1-8, 61-73** | |
| Тема № 11. Структура забезпечення інформаційної безпеки (Information Security Governance) | **14** | **4** | | **2** | | **8** | **1-8, 61-73** | |
| **Всього за семестр № 8:** | **180** | **44** | | **46** | | **90** | | |

## 2. Методичні вказівки до практичних занять

**Практичне заняття за темою № 1 «Основні положення щодо організації системи захисту інформації».**

Навчальна мета заняття: ознайомити здобувачів вищої освіти з основними положеннями з організації системи захисту інформації на об’єктах інформаційної діяльності

Час проведення: 6 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Умови безпеки інформації. Державна політика і система інформаційної безпеки в Україні.

2. Нормативно-правова база України в сфері інформаційної безпеки. Система захисту інформації у контексті системного мислення та системного підходу.

Література: [1-8].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 1. Нагадати основні визначення. Детально розглянути матеріал лекції 1. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.

15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**ІІІ. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу: з використанням ресурсів Internet знайти нові, нещодавно прийняті, нормативно-правові акти в сфері інформаційної безпеки. Оголосити тему наступного заняття.

**Теми цільових виступів**

1. Що розуміється під терміном "інформація", і які її, істотні з погляду захисту, властивості?
2. Які є види інформації за режимом доступу?
3. У чому суть так званої парадигми захисту інформації?
4. Яким чином парадигма захисту інформації враховує основні інформаційні загрози?
5. Якими чинниками обумовлюється розвиток в сфері інформаційної безпеки в Україні?
6. Які є основні загрози безпеці інформації в Україні?
7. Що є системою інформаційної безпеки?
8. На яких принципах реалізується державна політика в сфері інформаційної безпеки?
9. Хто виступає суб'єктами системи інформаційної безпеки України?
10. Що складає правову основу технічного захисту інформації в Україні?
11. Як можна розділити нормативно-правову і методичну базу в сфері інформаційної безпеки з урахуванням сфери застосування?
12. Що таке "інформаційна система"?
13. Що таке інформаційна система, і якими є її властивості?
14. У чому полягають ключові характеристики системного мислення та системного підходу?
15. Якою є ієрархія за рівнем узагальнення і складності об’єктів узагальненої інформаційно-телекомунікаційної системи?
16. Як можна представити ієрархію за рівнем узагальнення і складності?
17. Як можна застосувати ключові характеристики системного мислення та системного підходу до моделі мережі взаємин CITS-ISCS?

**Теми рефератів**

1. Види інформації за режимом доступу.
2. Стан забезпечення інформаційної безпеки в Україні.
3. Інформаційна система і її властивості.
4. Ключові характеристики системного мислення та системного підходу до моделі мережі взаємин CITS-ISCS.

**Практичне заняття за темою № 2 «Визначення інформаційних ресурсів, що підлягають захисту».**

Навчальна мета заняття: докладно розглянути порядок визначення інформаційних ресурсів, що підлягають захисту на об’єктах інформаційної діяльності.

Час проведення: 6 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Державна таємниця і конфіденційна інформація, що є власністю держави. Недержавна конфіденційна і відкрита інформація, що потребує захисту.
2. Дослідження структури і умов функціонування інформаційної системи організації. Модель системи об'єктів захисту.

Література: [1-8].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 2. Нагадати основні визначення. Детально розглянути матеріал лекції 2. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.

13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**ІІІ. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. Якими є основні кроки у визначенні інформаційних ресурсів, які підлягають захисту?
2. Що є об'єктом обов'язкового захисту інженерно-технічними заходами?
3. Які основні поняття державної таємниці і конфіденційної інформації, що є власністю держави?
4. Що можна віднести до недержавної конфіденційної і відкритої інформації, яка потребує захисту, і як це зробити?
5. Який можливий порядок проведення експертизи з метою визначення Переліку конфіденційних відомостей організації?
6. На яких носіях може існувати інформація, що потребує захисту?
7. Які вирішуються задачі при обстеженні інформаційної системи організації?
8. Яке значення мають терміни: виділений об'єкт, контрольована зона, категоріювання об'єкту, основні технічні засоби, допоміжні технічні засоби і системи?
9. Що може належати до основних і допоміжних технічних засобів і систем?
10. Які є вимоги до опису компонентів автоматизованої системи і технології обробки інформації?
11. Як можна представити модель системи інформаційних об'єктів захисту?
12. Як визначаються вагові коефіцієнти в моделі системи інформаційних об'єктів захисту?
13. Які документи необхідно мати після проведення робіт відповідно до першого етапу побудови системи захисту інформації?

**Теми рефератів**

1. Недержавна конфіденційна і відкрита інформації, яка потребує захисту.
2. Основні і допоміжні технічні засоби і системи.
3. Модель системи інформаційних об'єктів захисту.
4. Перший етап побудови системи захисту інформації.

**Практичне заняття за темою № 3. Виявлення повної множини загроз безпеки інформаційним ресурсам, які підлягають захисту**

Навчальна мета заняття: розглянути класифікацію загроз та джерел загроз інформації, технічні канали витоку інформації та НСД в комп'ютерних системах; окрему модель загроз та порушника.

Час проведення: 6 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Класифікація загроз інформації. Технічні канали витоку інформації та

НСД в комп'ютерних системах.

2. Окрема модель загроз. Джерела загроз і окрема модель порушника.

Література: [1-8].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 3. Нагадати основні визначення. Детально розглянути матеріал лекції 3. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**III. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. Як можна класифікувати загрози інформації?
2. Що є технічними каналами витоку інформації?
3. Як можна класифікувати технічні канали витоку інформації?
4. Як за допомогою схеми можна представити можливі канали витоку і несанкціонований доступ до інформації в типовому одноповерховому приміщенні?
5. Як можна описати і представити загрози в окремій моделі загроз?
6. Які розділи доцільно включити в окрему модель загроз об'єкту інформаційної діяльності?
7. Яка класифікація і перелік джерел загроз інформаційної безпеки?
8. Яким методом можна провести ранжирування джерел загроз інформаційної безпеки?
9. Яка класифікація використовується при створенні окремої моделі порушника?
10. Які документи необхідно мати після проведення робіт відповідно до другого етапу побудови системи захисту інформації, і який їх зміст?

**Теми рефератів**

1. Класифікація загроз інформації.
2. Технічні канали витоку інформації.
3. Загрози в окремій моделі загроз.
4. Класифікація і перелік джерел загроз інформаційної безпеки.
5. Окрема модель порушника.

**Практичне заняття за темою № 4. Проведення оцінки уразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз**

Навчальна мета заняття: ознайомити з можливими методиками оцінки вразливості і ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз.

Час проведення: 4 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Оцінка вразливості інформаційних ресурсів.
2. Оцінка ризиків для інформаційних ресурсів.

Література: [1-8].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 4. Нагадати основні визначення. Детально розглянути матеріал лекції 4. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**III. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. Яка класифікація і перелік уразливостей інформаційних ресурсів?
2. Яким методом можна провести ранжирування вразливостей інформаційних ресурсів?
3. Як можна представити і показати модель дії загроз на множину об'єктів захисту та існуючої системи захисту інформації?

4. Як визначаються вагові коефіцієнти в моделі дії загроз на множину об'єктів захисту та існуючої системи захисту інформації?
5. Яким чином визначаються інформаційні ризики, і здійснюється управління ними?
6. Які документи необхідно мати після проведення робіт відповідно до третього етапу побудови системи захисту інформації, і який їх зміст?

**Теми рефератів**

1. Класифікація і перелік уразливостей інформаційних ресурсів.
2. Методи ранжирування вразливостей інформаційних ресурсів.
3. Методи визначення інформаційних ризиків.

**Практичне заняття за темою № 5. Методи та засоби захисту інформації**

Навчальна мета заняття: нагадати основні методи та засоби захисту інформації від витоку технічними каналами, розглянути національні критерії захисту інформації від НСД в комп'ютерних системах.

Час проведення: 4 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Методи і засоби захисту інформації від витоку по технічних каналах.
2. Основні положення "Критеріїв оцінки захищеності інформації в комп'ютерних системах від НСД ".

Література: [1-9].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 5. Нагадати основні визначення. Детально розглянути матеріал лекції 5. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.

5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**III. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. Якими можуть бути організаційні заходи захисту інформації від витоку технічними каналами?
2. Якими можуть бути первинні технічні заходи захисту інформації від витоку технічними каналами?
3. На яких принципах базуються основні технічні заходи захисту інформації від витоку технічними каналами, і яка їх суть?
4. Що належить до спеціальних засобів ТЗІ?
5. Що передбачають основні технічні заходи?
6. Яка суть заходів щодо блокування ТКВІ з використанням пасивних засобів?
7. Яка суть заходів щодо блокування ТКВІ з використанням активних засобів?
8. Яка суть заходів щодо виявлення портативних електронних пристроїв перехоплення інформації?
9. Якими є основні поняття теорії захисту інформації в комп'ютерних системах?
10. Які існують підходи в представленні моделі довільної комп'ютерної системи, і в чому їх суть?
11. На рішення яких проблем спрямовані стандарти інформаційної безпеки?
12. Які стандарти інформаційної безпеки найбільш відомі?
13. Які поняття об'єкту інформаційного обміну використовуються в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД" і з чого складається загальна оцінка рівня безпеки системи?

14. Які послуги передбачають критерії конфіденційності в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД", і в чому їх суть?
15. Які послуги передбачають критерії цілісності в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД", і в чому їх суть?
16. Які послуги передбачають критерії доступності в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД", і в чому їх суть?
17. Які послуги передбачають критерії спостереженості в "Критеріях оцінки захищеності інформації в комп'ютерних системах від НСД", і в чому їх суть?
18. Які розділи включають критерії гарантій "Критерії оцінки захищеності інформації в комп'ютерних системах від НСД"?
19. Що є стандартними функціональними профілями захищеності, і як вони описуються?

**Теми рефератів**

1. Організаційні заходи захисту інформації від витоку технічними каналами.
2. Технічні заходи захисту інформації від витоку технічними каналами.
3. Спеціальні засоби ТЗІ.
4. Основні поняття теорії захисту інформації в комп'ютерних системах.
5. Стандарти інформаційної безпеки.

**Практичне заняття за темою № 6. Захист інформації в комп'ютерних системах від несанкціонованого доступу**

Навчальна мета заняття: розглянути основні положення міжнародного стандарту ISO/IEC 15408 та національного стандарту США NIST Special Publication 800-33.

Час проведення: 4 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Основні положення стандарту ISO/IEC 15408.
2. Базова технічна модель IT-безпеки відповідно до NIST Special Publication 800-33.

Література: [1-8].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 6. Нагадати основні визначення. Детально розглянути матеріал лекції 6. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).

3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**III. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. Які ключові поняття використовуються в "Загальних критеріях"?
2. Як можна представити схему оцінки безпеки ІТ-продукту на основі "Загальних критеріїв"?
3. Якою є структура і розділи Профілю захисту, Проекту захисту "Загальних критеріїв"?
4. Якою є ієрархія і ознаки поділу функціональних вимог "Загальних критеріїв"?
5. Якою є таксономія класів функціональних вимог "Загальних критеріїв", і в чому їх суть?
6. Якою є таксономія сімейств функціональних вимог для всіх класів "Загальних критеріїв"?

7. Що включає розділ "Загальних критеріїв", який описує вимоги адекватності?
8. Якою є таксономія вимог адекватності "Загальних критеріїв", і в чому їх суть?
9. Як характеризуються стандартні рівні адекватності "Загальних критеріїв"?
10. Якою є головна мета і завдання IT-безпеки відповідно до NIST Special Publication 800-33?
11. Як залежать одна від одної задачі IT-безпеки?
12. Яким чином можна представити модель взаємодії послуг безпеки в IT-системах?
13. У чому полягає суть послуг безпеки в IT-системах?
14. Які потрібні послуги для вирішення задач доступності і цілісності в моделі взаємодії послуг безпеки в IT-системах?
15. Які потрібні послуги для вирішення задач спостереженості і гарантій в моделі взаємодії послуг безпеки в IT-системах?
16. Як можна представити взаємну залежність розподілених сервісів безпеки відповідно до NIST Special Publication 800-33?
17. За рахунок чого можуть бути збільшені гарантії системи відповідно до NIST Special Publication 800-33?
18. У чому полягає суть концепції доменів безпеки для IT-безпеки мереж?
19. Яким є алгоритм зменшення інформаційних ризиків при наявності навмисних і ненавмисних джерел загроз?

**Теми рефератів**

1. Складання схеми оцінки безпеки IT-продукту на основі "Загальних критеріїв".
2. Головна мета і завдання IT-безпеки відповідно до NIST Special Publication 800-33.
3. Задачі IT-безпеки.
4. Алгоритм зменшення інформаційних ризиків при наявності навмисних і ненавмисних джерел загроз.

**Практичне заняття за темою № 7. Політика інформаційної безпеки**

Навчальна мета заняття: розглянути основні положення та зміст документів політики безпеки організації (підрозділу).

Час проведення: 4 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Загальні положення щодо політики безпеки.
2. Зміст основних документів політики безпеки.

Література: [1-9].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 7. Нагадати основні визначення. Детально розглянути матеріал лекції 7. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**III. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. Яку роль в СЗІ виконує політика безпеки, і яка модель організацій з позиції їх зрілості в сфері інформаційної безпеки запропонована Carnegie Mellon University?
2. У вигляді яких документів доцільно оформляти політику безпеки організації?
3. Які цілі і завдання політики безпеки організації?

4. Які обов'язки керівників і співробітників організації в сфері інформаційної безпеки?
5. Які можуть бути вимоги політики безпеки організації щодо забезпечення фізичної безпеки комп'ютерної системи?
6. Які можуть бути загальні вимоги політики безпеки організації щодо управління і використання комп'ютерної системи?
7. Які можуть бути правила безпеки при використанні зовнішніх ресурсів (Internet)?
8. Які можуть бути правила безпеки при використанні електронної пошти?
9. Які можуть бути вимоги політики безпеки організації щодо організації антивірусного захисту комп'ютерної системи?
10. Які можуть бути вимоги політики безпеки організації щодо управління і експлуатації криптографічних систем в комп'ютерній системі?
11. Які можуть бути правила впровадження програмного забезпечення в контексті безпеки?
12. Що є зобов'язанням виконання Політики безпеки організації?
13. Як можна визначити порядок впровадження і контролю виконання політики безпеки?
14. Яким може бути порядок перегляду політики безпеки?

**Теми рефератів**

1. Документальне оформлення політики безпеки організації.
2. Цілі і завдання політики безпеки організації.
3. Загальні вимоги політики безпеки організації щодо управління і використання комп'ютерної системи.
4. Правила безпеки при використанні зовнішніх ресурсів (Internet).
5. Порядок перегляду політики безпеки.

**Практичне заняття за темою № 8. Розробка проекту системи захисту інформації**

Навчальна мета заняття: ознайомити з можливою моделлю простору заходів і засобів захисту інформації, критеріями і особливості проектування оптимальної системи захисту інформації, оформленням відповідних документів.

Час проведення: 4 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Модель простору заходів і засобів захисту.
2. Критерій і особливості проектування оптимальної системи захисту інформації. Технічне завдання на розробку СЗІ і План захисту інформації.

Література: [1-9].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 8. Нагадати основні визначення. Детально розглянути матеріал лекції 8. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**III. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. У вигляді якої структури можна представити простір СЗІ, і які її елементи?
2. Яке завдання розв'язується при оптимізації СЗІ, і за якими критеріями?
3. Які особливості і послідовність задач, що вирішуються при проектуванні СЗІ?
4. Які розділи передбачає Технічне завдання на розробку СЗІ і План захисту інформації?

5. Що можна передбачити як організаційні заходи щодо реалізації проекту (плану) захисту інформації?

**Теми рефератів**

1. Характеристика простору СЗІ.
2. Оптимізація СЗІ.
3. Зміст технічного завдання на розробку СЗІ і Плану захисту інформації.

**Практичне заняття за темою № 9. Впровадження, визначення якості і управління системою захисту інформації**

Навчальна мета заняття: розглянути порядок реалізації проекту (плану) захисту інформації, визначення якості реалізованої системи захисту та контролю за функціонуванням.

Час проведення: 4 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Реалізація проекту (плану) захисту інформації.
2. Визначення якості реалізованої системи захисту. Контроль функціонування і управління системою захисту.

Література: [1-9].

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 9. Нагадати основні визначення. Детально розглянути матеріал лекції 9. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.

7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п'ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**III. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. Що можна передбачити як контрольно-правові, профілактичні і інженерно-технічні заходи щодо реалізації проекту (плану) захисту інформації?
2. Який зміст етапу "визначення якості реалізованої системи захисту"?
3. Які види державної експертизи і порядок її організації та проведення?
4. Які види атестації і порядок її організації та проведення?
5. Які документи необхідно мати після проведення робіт відповідно до шостого етапу побудови системи захисту інформації, і який їх зміст?
6. У чому суть контрольно-інспекційної роботи з питань ТЗІ щодо суб'єктів системи ТЗІ?

**Теми рефератів**

1. Контрольно-правові, профілактичні і інженерно-технічні заходи щодо реалізації проекту (плану) захисту інформації.
2. Визначення якості реалізованої системи захисту.
3. Види державної експертизи і порядок її організації та проведення.
4. Суть контрольно-інспекційної роботи з питань ТЗІ щодо суб'єктів системи ТЗІ

**Практичне заняття за темою № 10. Нормативно-правова база США щодо забезпечення інформаційної безпеки**

Навчальна мета заняття: розглянути основні нормативно-правові акти США у сфері управління та організації інформаційної безпеки.

Час проведення: 2 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Поняття кіберпростору. Огляд основних законів щодо інформаційної безпеки кіберпростору.

2. Federal Information Security Management Act of 2002, FISMA. Класифікація нормативних документів з інформаційної безпеки.

**Література:** [1-8, 61-73] зі списку літератури, наведеної у методичних матеріалах до практичних занять.

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 10. Нагадати основні визначення. Детально розглянути матеріал лекції 10. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру

набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**ІІІ. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу, оголосити тему наступного заняття.

**Теми цільових виступів**

1. Якими основними ознаками характеризується кіберпростір?
2. Що таке юрисдикція?
3. Яким є правовий режим Інтернет?
4. Який закон США вперше містив визначення терміну «електронний підпис»?
5. Який закон США вперше дав офіційне тлумаченням терміну «інформаційна технологія»?
6. Який закон США відображає намір уряду США захистити власні комп'ютерні мережі?
7. Яка організація безпосередньо розробляє різні типи документів з інформаційної безпеки?
8. Які типи документів з інформаційної безпеки публікує Computer Security Division?

**Теми рефератів**

1. Кіберпростір: визначення, ознаки.
2. Правовий режим Інтернет.
3. Нормативно-правове забезпечення інформаційної безпеки США.

**Практичне заняття за темою № 11. Структура забезпечення інформаційної безпеки (Information Security Governance)**

Навчальна мета заняття: розглянути структуру забезпечення інформаційної безпеки США, державні механізми у сфері управління та організації інформаційної безпеки.

Час проведення: 2 год.

Місце проведення: згідно з розкладом.

Навчальні питання

1. Загальні вимоги забезпечення інформаційної безпеки. Складові забезпечення інформаційної безпеки.
2. Проблеми та шляхи їх вирішення у забезпеченні інформаційної безпеки.

**Література:** [1-8, 61-73] зі списку літератури, наведеної у методичних матеріалах до практичних занять.

**План проведення заняття:**

**І. Порядок проведення вступу до заняття.**

Перевірити згідно журналу навчальної групи наявність здобувачів вищої освіти. Оголосити тему заняття, навчальну мету і план заняття.

**ІІ. Порядок проведення основної частини заняття.**

Провести опитування за контрольними питаннями до лекції 11. Нагадати основні визначення. Детально розглянути матеріал лекції 11. Обговорити питання, розібрати матеріал лекції, що викликає складність в засвоєнні.

1. Здобувачі вищої освіти заздалегідь отримують перелік питань для підготовки (див. наприкінці кожної лекції) та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є викладач).

3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього викладач задає питання, номер якого відповідає названому доповідачами числу у списку питань викладача. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене викладачем питання. В цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання викладача протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання у відповідності до відповіді доповідачів.
6. Опоненти задають питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти задають питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Викладач задає контрольне питання за розглянутим питанням кожній з команд.
11. Викладач оцінює якість роботи кожної з команд.
12. Критерії оцінювання (за п’ятибальною шкалою кожний):
    - повнота та аргументованість відповідей;
    - робота в команді;
    - дотримання правил етикету.
13. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
14. По закінченні гри підбиваються підсумки.
15. Члени команди, яка набрала найбільшу кількість балів протягом гри отримують призові бали на модульному тесті. Команда яка протягом семестру набрала найбільшу кількість балів протягом усіх ігор отримує призові бали на заліковому тесті.

**III. Порядок проведення заключної частини заняття**

Підвести підсумки заняття, оголосити оцінки, задати завдання на самостійну роботу.

**Теми цільових виступів**

1. Які інституції і яким чином визначають вимоги з ІБ та впливають на забезпечення інформаційної безпеки федеральних організацій США?
2. Якими є основні види діяльності щодо інтегрування заходів інформаційні безпеки в загальну структуру організації США?
3. У чому суть стратегічного планування інформаційної безпеки у федеральній агенції США?
4. Якими можуть бути структури забезпечення ІБ у федеральній організації США?
5. Які типові посади (ролі), що мають відношення до ІБ, характерні для більшості організацій?

6. Хто такий Федеральний Корпоративний Архітектор і яке відношення він має до ІБ організацій?
7. У чому полягає політика інформаційної безпеки установи США?

**Теми рефератів**

1. Стратегічне планування інформаційної безпеки у федеральній агенції США.
2. Державно-приватне партнерство у забезпеченні інформаційної безпеки у США.
3. Структури забезпечення ІБ у федеральній організації США.
4. Політика інформаційної безпеки установи США.

## 3. Рекомендована література (основна, допоміжна), інформаційні ресурси в інтернеті

### 3.1 Основна:


1. Управління інформаційною безпекою: конспект лекцій: навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С.О. Носок, О.М. Фаль, В.М. Ткач. Київ: КПІ ім. Ігоря Сікорського, 2021. – 258 с. URL:https://ela.kpi.ua/handle/123456789/43377.
2. Навчальний посібник для учасників тренінгу «Розробка та впровадження системи управління безпекою інформації». – Київ: BAITE, 2021. – 138 с.
3. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с. URL: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf
4. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.: іл. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/%d0%86%d0%bd%d1%84%d0%be%d1%80%d0%bc.%20%d0%b1%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%d0%b0%20%d0%b4%d0%b5%d1%80%d0%b6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
5. Захист інформації в комп'ютерних системах: підручник для студентів інженерно-технічного факультету ДВНЗ «УжНУ»; уклад.: Гапак О.М., Балога С.І. Ужгород, 2021. – 184 с. URL: https://uzhnu.edu.ua/en/infocentre/get/42935
6. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с., іл.160.
7. Бабак В.П. Теоретичні основи захисту інформації: підручник / В.П. Бабак, А.А. Ключников; НАН України, Ін-т проблем безпеки АЕС. Чорнобиль (Київ.обл.): Ін-т проблем безпеки АЕС, 2012. 776 с.
8. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД: навч. посіб. / М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев // За ред. ак. МАІ М.В. Захарченка. – Одеса: ОНАЗ ім. О.С. Попова, 2011. – 168 с.

9. Концепція технічного захисту інформації в Україні. Постанова КМУ від 08.10.1997 № 1126.
10. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України від 23.02.2006 № 3475-IV.
11. Про інформацію. Закон України від 02.10.1992 № 2657-XII.
12. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР.
13. Про державну таємницю. Закон України від 21.01.1994 № 3855-XII.
14. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI.
15. Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229.
16. Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281.
17. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.1996 № 423.
18. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.1996 № 511.
19. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.1997 № 200.
20. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
21. ДСТУ 1.5:2003 Правила побудови, викладання, оформлення та вимоги до змісту нормативних документів.
22. ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2015, IDT) URL:http://arm.ho.ua/SACSN/ISO_IEC_27002_2015.pdf.
23. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795.
24. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27001:2013/Cor 2:2015, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. URL:https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf
25. ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT). Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. URL:http://online.budstandart.com/ua/catalog/doc-page?id_doc=66911
26. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. URL:http://online.budstandart.com/ua/catalog/doc-page?id_doc=85797
27. ДСТУ ISO/IEC 27007:2018 (ISO/IEC 27007:2017, IDT) Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування

інформаційною безпекою. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80303
28. ДСТУ ISO/IEC 27009:2018 (ISO/IEC 27009:2016, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80305
29. ДСТУ ISO/IEC 27010:2018 (ISO/IEC 27010:2015, IDT) Інформаційні технології. Методи захисту. Керування інформаційною безпекою для міжгалузевих та міжорганізаційних комунікацій. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80308
30. ДСТУ ISO/IEC 27011:2018 (ISO/IEC 27011:2016, IDT) / Поправка № 1:2019 (ISO/IEC 27011:2016/Cor 1:2018, IDT). Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування інформаційною безпекою на основі ISO/IEC 27002. URL:http://online.budstandart.com/ua/catalog/doc-page?id_doc=85806
31. ДСТУ ISO/IEC 27011:2018 (ISO/IEC 27011:2016, IDT) Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування інформаційною безпекою на основі ISO/IEC 27002. URL:http://online.budstandart.com/ua/catalog/doc-page?id_doc=85806
32. ДСТУ ISO/IEC 27013:2017(ISO/IEC 27013:2015, IDT) Інформаційні технології. Методи захисту. Настанови для інтегрованого впровадження ISO/IEC 27001 та ISO/IEC 20000-1. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=74956
33. ДСТУ ISO/IEC 27017:2017 (ISO/IEC 27017:2015, IDT) Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=67136
34. ДСТУ ISO/IEC 27018:2019 (ISO/IEC 27018:2019, IDT) Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85799
35. ДСТУ ISO/IEC 27019:2019 (ISO/IEC 27019:2017, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою для енергопостачальних організацій. URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=83587
36. ДСТУ ISO/IEC 27021:2018 (ISO/IEC 27021:2017, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги до компетенції для професіоналів з керування інформаційною безпекою. URL:http://online.budstandart.com/ru/catalog/doc-page.html?id_doc=80481
37. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). URL:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128
38. ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки. URL:http://online.budstandart.com/ua/catalog/doc-page?id_doc=85798

39. ДСТУ ISO/IEC TS 27034-5-1:2019 (ISO/IEC TS 27034-5-1:2018, IDT) Інформаційні технології. Захист застосунків. Частина 5-1. Структура даних керування протоколами та захистом застосунків. Схеми XML. URL:http://online.budstandart.com/ua/catalog/doc-page?id_doc=85801
40. НД ТЗІ 1.1-002-99.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
41. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
42. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.
43. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу "2".
44. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
45. НД ТЗІ 1.1-004-2003 Протидія технічним розвідкам. Терміни та визначення.
46. Перелік обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних. Постанова КМ України від 04.02.1998 № 121.
47. Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Постанова КМ України від 16.02.1998 № 180.
48. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Постанова КМ України від 16.11.2002 № 1772.
49. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМ України від 29.03.2006 № 373.
50. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.
51. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
52. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.
53. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
54. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1).
55. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).
56. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
57. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці", затверджене наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215.

58. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
59. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
60. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.

**3.2 Додаткова:**

61. Federal Information Security Management Act of 2002 (FISMA): Закон Федерального Уряду США по управлінню інформаційною безпекою.
62. National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology, October 2006.
63. National Institute of Standards and Technology Special Publication 800-64, Security Considerations in the Information System Development Life Cycle, Rev. 2, October 2008.
64. National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, October 2003.
65. NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model.
66. National Institute of Standards and Technology Special Publication 800-65, Integrating Information Security into the Capital Planning and Investment Control Process, January 2005.
67. National Institute of Standards and Technology Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002.
68. National Institute of Standards and Technology Special Publication 800-55, Security Metrics Guide for Information Technology Systems, Revision 1, July 2008.
69. National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems, February 2006.
70. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Contingency Planning for Information Technology Systems, June 2002.
71. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems, July 2002.
72. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-36, Guide to Selecting Information Technology Security Products, October 2003.
73. Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide, March 2008.

**3.3 Інформаційні ресурси в інтернеті:**

74. https://cip.gov.ua/ua
75. https://cert.gov.ua/
76. https://ssu.gov.ua/